УДК: 004.056.5 DOI: 10.53816/23061456_2021_9–10_72

ПОДХОД К КОНТРОЛЮ ДЕЙСТВИЙ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ В КРИТИЧЕСКИ ВАЖНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

AN APPROACH TO CONTROLLING THE ACTIONS OF PRIVILEGED USERS IN CRITICAL AUTOMATED SYSTEMS

Канд. техн. наук В.М. Зима, Р.О. Крюков

Ph.D. V.M. Zima, R.O. Kryukov

ВКА им. А.Ф. Можайского

Широкие полномочия привилегированных пользователей в критически важных автоматизированных системах (АС) дают возможность нейтрализовать некоторые функции контроля и защиты информации. При этом атаки со стороны привилегированных пользователей долгое время остаются незамеченными. Таким образом, преднамеренные или случайные действия привилегированных пользователей могут привести к нарушению или прекращению функционирования критически важных АС. В статье рассмотрены особенности реализации архитектуры системы контроля действий привилегированных пользователей. Представлен практический подход к обеспечению контроля действий привилегированных пользователей в критически важных АС, основанный на комплексном использовании различных механизмов защиты информации.

Ключевые слова: безопасность информации, средства защиты информации от несанкционированного доступа, система контроля действий администраторов, система обнаружения вторжений, система мониторинга событий информационной безопасности, администратор аудита, коллегиальное администрирование.

The extensive powers of privileged users in mission-critical automated systems (AS) enable them to neutralize some control and information protection functions. However, attacks by privileged users remain undetected for a long time. So, deliberate or accidental actions of privileged users can cause disruption or termination of critical AC. The article considers peculiarities of privileged user activity control architecture implementation. It presents a practical approach to controlling the actions of privileged users in a critical system, based on an integrated use of various information security mechanisms.

Keywords: information security, information security tools from unauthorized access, administrator action control system, intrusion detection system, information security event monitoring system, audit administrator, collegial administration.

Введение

При разработке подсистемы защиты большинства автоматизированных систем (АС) в модели угроз при систематизации нарушителей вводится ограничение, в соответствии с которым в качестве нарушителей не рассматриваются администраторы АС.

Данное ограничение, с одной стороны, базируется на том, что обслуживание технических и программных средств АС осуществляется кругом наиболее доверенных лиц, на которых распространяется система организационно-кадровых и режимных мер, а с другой — вызвано сложностью реализации полноценного контроля действий администраторов АС. Однако при этом не учитывается, что их преднамеренные или случайные действия могут привести к компрометации ее подсистемы защиты целиком. Для критически важных АС, нарушение или прекращение функционирования которых приводит к необратимым негативным последствиям, введение подобных ограничений является недопустимым, и контролю должны подлежать действия всех пользователей АС, включая действия ее администраторов [1–3].

Обеспечить полноценный контроль действий привилегированных пользователей возможно только на основе комплексного использования различных механизмов защиты информации, реализованных в системе контроля действий администраторов.

Общие сведения

Контроль действий администраторов в АС предполагает комбинирование следующих механизмов защиты:

1) регистрация всех событий, связанных с действиями администраторов, в журналах аудита;

2) анализ журналов аудита в режиме реального времени с помощью системы обнаружения вторжений (СОВ) или системы мониторинга событий информационной безопасности (SIEM-системы — от англ. Security Information And Event Management);

3) контроль функций администрирования, передаваемых исполняемых команд, а также утечек закрытой информации и блокировка всех несоответствий политике безопасности с помощью СОВ на основе сигнатурного и поведенческого анализа;

4) реализация средств формирования и проверки электронной подписи для обеспечения подлинности записей журналов аудита;

5) разделение полномочий администраторов с выделением контролирующей роли — администратора аудита;

6) введение коллегиального администрирования для наиболее критичных операций, например, операций, связанных с созданием учетных записей привилегированных пользователей или назначением привилегированных ролей;

7) использование программных агентов контроля на АРМ контролируемых администраторов и/или сервера-посредника как единой точки доступа к функциям администрирования, обеспечивающего усиленную аутентификацию администраторов, контроль доступа, видео-запись графических сессий (например, для протокола RDP), а также запись текстовых сессий (например, для протокола SSH).

Перечисленные механизмы защиты могут быть реализованы в различных подсистемах АС, однако, на практике максимальная результативность контроля действий привилегированных пользователей достигается при объединении данных функций в единую систему контроля действий администраторов (СКДА).

Архитектура СКДА

СКДА целесообразно создавать по архитектуре «консоль–менеджер (модуль управления)–агент (модуль контроля)». Менеджер (модуль управления) может быть выделен в специализированный сервер-посредник или сервер приложений, и включать хранилище данных [4]. В зависимости от особенностей реализации архитектуры «консоль–менеджер (модуль управления)–агент (модуль контроля)» можно выделить следующие типы СКДА:

1) СКДА на основе сервера-посредника, устанавливаемого в «разрыв» между управляющим сегментом ЛВС и управляемыми сегментами сети АС без использования агентов, функционирующих на АРМ контролируемых администраторов (рис. 1). В этом случае необходимо, чтобы модуль контроля и, как правило, модуль управления функционировали на сервере-посреднике. Модуль контроля настраивается через модуль управления, а взаимодействие администратора контроля (аудита) с модулем управления по сети выполняется через графическую консоль, в качестве которой разумно использовать Web-браузер;

2) СКДА, которые не требуют разделения управляющего и управляемых сегментов с по-

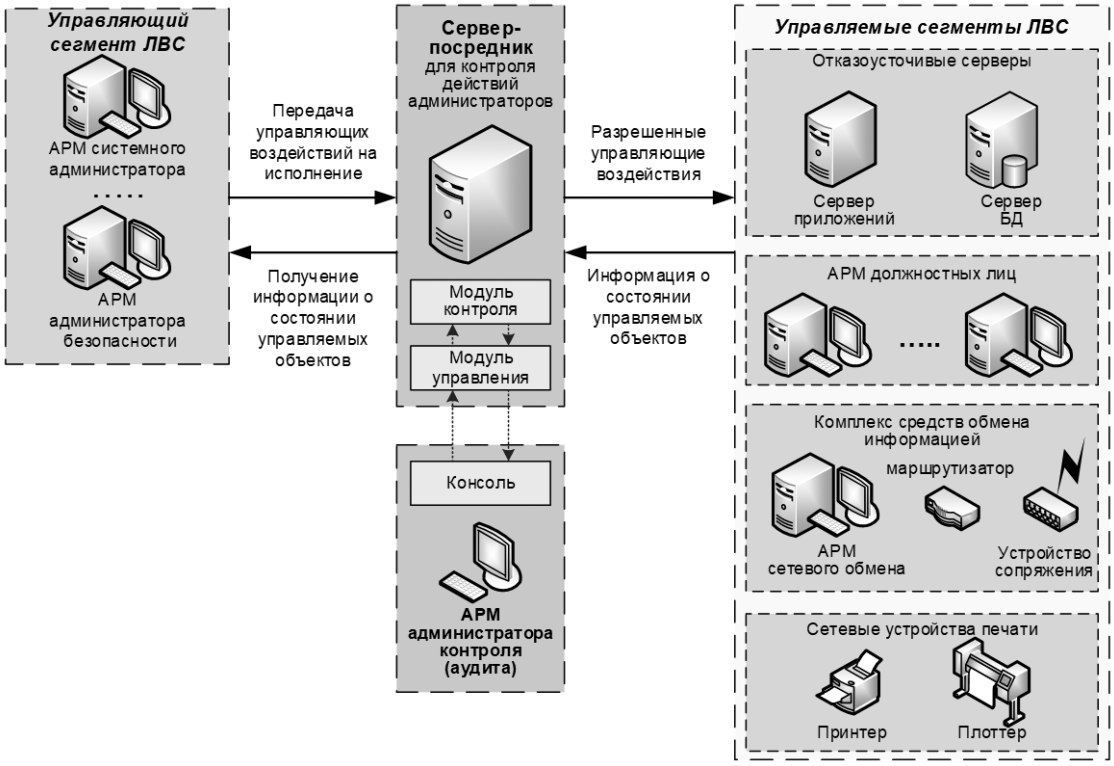

Рис. 1. Архитектура СКДА на основе сервера-посредника без использования агентов

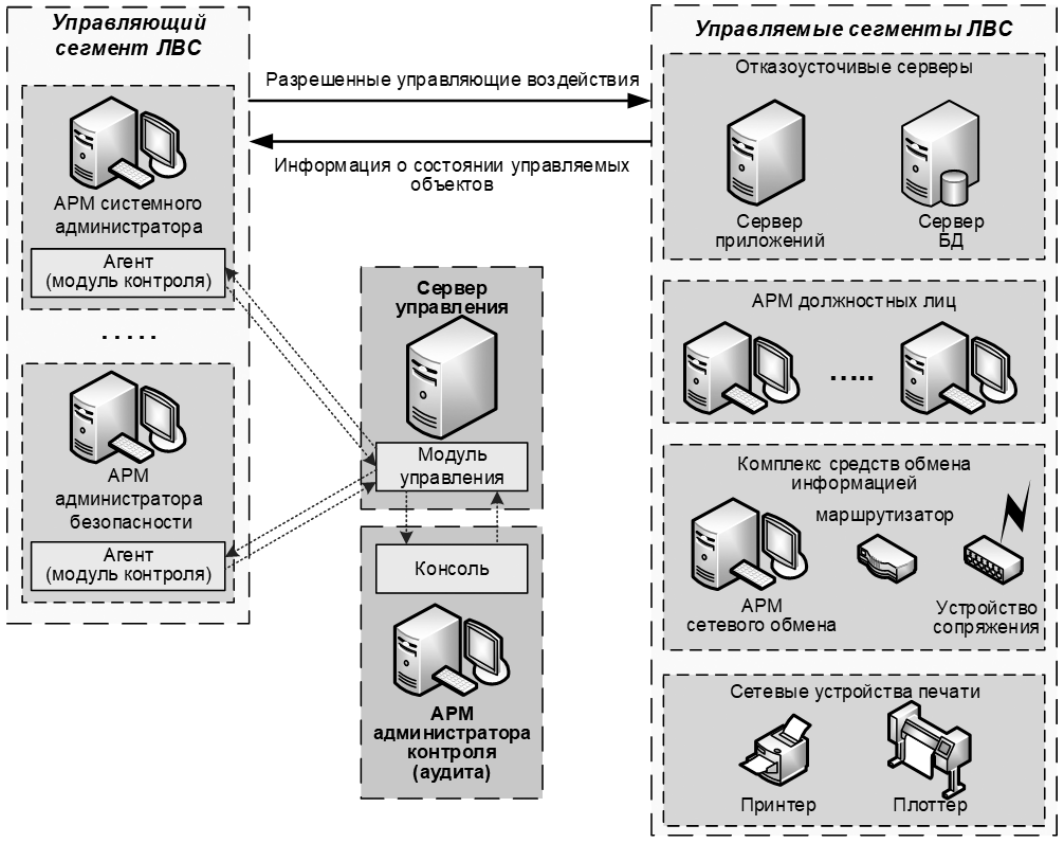

Рис. 2. Архитектура СКДА, не требующая разделения управляющего и управляемых сегментов с помощью сервера-посредника

мощью сервера-посредника, функционирующие на основе программных агентов на АРМ контролируемых администраторов. В этом случае модули контроля должны функционировать как агенты на АРМ контролируемых администраторов (рис. 2.) Агенты (модули контроля) настраиваются через модуль управления, для которого выделяется отдельный сервер управления. Взаимодействие администратора контроля (аудита) с модулем управления по сети также выполняется через графическую консоль (Web-браузер);

3) СКДА, построенные по совмещенной архитектуре, при которой используется как сервер-посредник в «разрыве» между управляющим и управляемыми сегментами ЛВС, так и агенты, установленные на АРМ администраторов (рис. 3). В этом случае функционал агентов на АРМ контролируемых администраторов и модуля контроля на сервере-посреднике не должен пересекаться, например, агенты могут выполнять анализ журналов аудита на АРМ контролируемых администраторов в режиме реального времени, а модуль контроля на сервере-посреднике — осуществлять контроль функций администрирования и передаваемых исполняемых команд с блокировкой всех несоответствий политике безопасности.

Наиболее защищенными, надежными, масштабируемыми и отличающимися более низкой сложностью реализации являются СКДА, не требующие разделения управляющего и управляемых сегментов с помощью сервера-посредника (рис. 2). Это связано со следующими особенностями СКДА, функционирующих на основе агентов на АРМ контролируемых администраторов без использования сервера-посредника:

– сервер-посредник легко обойти при наличии у контролируемых администраторов физического доступа к АРМ и серверам в управляемом сегменте, так как они могут под своими учетными записями войти в систему через любой АРМ и сервер управляемого сегмента;

– отсутствие сервера-посредника в «разрыве» сети повышает надежность всей системы защиты и не создает проблем с масштабируемостью сетевой инфраструктуры;

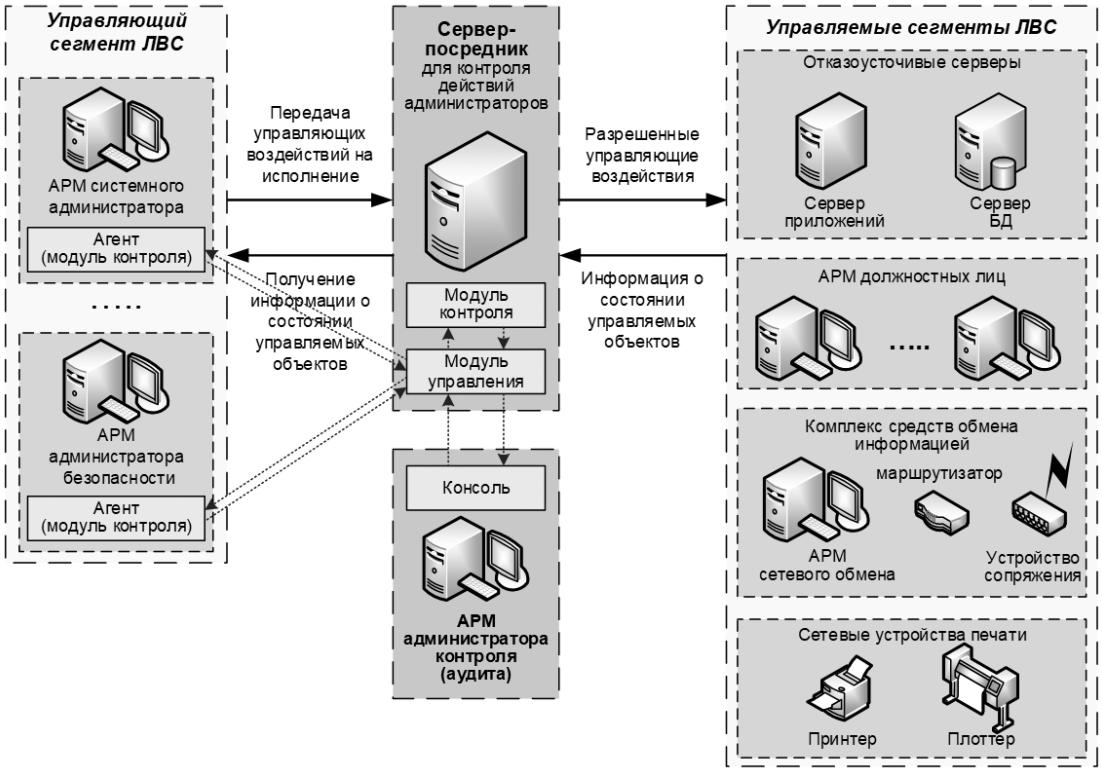

Рис. 3. Совмещенная архитектура СКДА, при которой используется как сервер-посредник в «разрыве» между управляющим и управляемыми сегментами ЛВС, так и агенты, установленные на АРМ администраторов

– СКДА без сервера-посредника не требуют доработок для совместимости с базовым протоколом доменной аутентификации Kerberos, так как используется реализация этого протокола на уровне операционной среды АРМ и серверов, например, ОС Astra Linux SE, и сервер-посредник не блокирует в «разрыве» сети протокол аутентификации и другие служебные протоколы;

– сервер-посредник должен перехватывать все сессии администраторов и создавать новые. Соответственно, при отсутствии сервера-посредника нет необходимости в дополнительной реализации в составе СКДА как стандартных протоколов администрирования, например, SSH (Secure Shell), так и протоколов администрирования, разработанных для специального программного обеспечения (СПО), например, на основе REST API (Representational State Transfer Application Programming Interface).

По перечисленным причинам СКДА, которые требуют сервера-посредника как единой точки доступа к функциям администрирования, используют, в основном, при контроле доступа к АС удаленных администраторов из информационно-телекоммуникационная сеть общего пользования (ИТКС ОП) Интернет, что запрещено для критических объектов автоматизации. В СКДА, построенных по совмещенной архитектуре, при которой используется как сервер-посредник в «разрыве» между управляющим и управляемыми сегментами ЛВС, так и агенты, сервер посредник, как правило, также применяется только для контроля доступа к АС удаленных администраторов из ИТКС ОП Интернет.

Недостатком СКДА на основе агентов, не требующих разделения управляющего и управляемых сегментов с помощью сервера-посредника, является то обстоятельство, что для максимальной защищенности необходима установка агентов не только на АРМ контролируемых администраторов, но и на всех АРМ и серверах управляемого сегмента, к которым у этих администраторов имеется физический доступ. Но это не снижает их преимущества, так как агенты СКДА могут быть интегрированы в датчики узловых СОВ или агенты средств антивирусной защиты (САВЗ).

Технологический фундамент для обнаружения атак в режиме реального времени, включая атаки со стороны администраторов, составляют функции динамического контроля эталонного состояния элементов компьютерной системы:

– проверка соответствия элементов компьютерной системы признакам, характерным для процесса реализации атак и отклонения от эталонного режима функционирования;

– проверка соответствия текущих характеристик информационных и программных объектов эталонным характеристикам, что реализуется на основе контроля целостности с помощью электронной подписи и криптографического хеширования.

Проверка соответствия элементов компьютерной системы признакам, характерным для процесса реализации атак и отклонения от эталонного режима функционирования, базируется на трех подходах:

– на сигнатурном анализе, в процессе которого осуществляется поиск признаков, характерных для процесса реализации атак;

– на поведенческом анализе, в процессе которого осуществляется поиск признаков, характерных для отклонения элементов системы от эталонного режима функционирования;

– на анализе журналов регистрации, в процессе которого осуществляется поиск признаков, как атак, так и аномалий в поведении системы, но на основе сбора и обработки информации, протоколируемой используемыми средствами защиты, СПО, ОС, сервисами, активным коммуникационным оборудованием и др. элементами АС.

В основу построения СКДА должны быть положены как методы обнаружения атак на основе анализа журналов регистрации, так и методы сигнатурного и поведенческого анализа, реализуемые в составе СОВ [5]. Целесообразна также реализация аппарата электронной подписи для обеспечения подлинности записей журналов аудита [6]. Кроме того, важны организационно-технические меры, связанные с разделением полномочий администраторов и введением коллегиального администрирования.

Разделение полномочий администраторов и введение коллегиального администрирования

Разделение полномочий администраторов АС предполагает назначение различным адми-

нистраторам непересекающихся функций администрирования и организацию контроля их действий. Например, в АС могут использоваться следующие категории учетных записей администраторов:

– операторы пунктов контроля и управления;

– системные администраторы;

– администраторы информационных подсистем;

– администраторы безопасности;

– администраторы аудита.

Администраторы аудита назначаются для контроля действий остальных администраторов, а также мониторинга доступа к защищаемым ресурсам и средствам администрирования. Записи в журналах регистрации с информацией об обращениях всех должностных лиц к защищаемым ресурсам и функциям администрирования должны быть подписаны электронной подписью для обеспечения их подлинности.

Обработка защищаемой информации в АС должна осуществляться только с использованием учетных записей, отнесенных к категориям пользователей АС.

В методическом документе ФСТЭК России «Меры защиты информации в государственных информационных системах» [7] меры по разделению полномочий администраторов АС, перечисленные в приказе ФСТЭК России № 17 от 2013 года с изменениями от 2017 года [8], детализируются в составе мер по управлению доступом субъектов доступа к объектам доступа (УПД) под номером 4 (УПД.4 — разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы).

Коллегиальное администрирование предполагает реализацию в системе защиты таких механизмов, при которых обеспечивается выполнение отдельных критичных функций администрирования только коллегиально, т.е. совместно двумя или более администраторами. При этом модель нарушителя базируется на положении, что создание коалиций внутренних нарушителей среди администраторов, то есть их объединения (сговора) и целенаправленных действий по преодолению системы защиты исключено.

Технически механизмы коллегиального администрирования могут быть реализованы двумя способами:

1) разделением критичной функции администрирования на несколько этапов, при котором за каждый этап отвечает отдельный администратор, например:

– разделением функции управления учетными записями пользователей на этапе создания учетных записей пользователей и этапе назначения полномочий и прав с последующей активацией этих учетных записей для возможности входа в систему;

– разделением функции вывода информации из АС на отчуждаемый машинный носитель информации (МНИ) на этапе подготовки списка выводимых документов и этапе непосредственного вывода документов из подготовленного списка на отчуждаемый МНИ;

2) возможностью доступа к критичной функции администрирования, например, функции назначения прав доступа, только после входа в систему двух или более имеющих на это полномочия администраторов, один из которых непосредственно выполняет эту функцию, а другие контролируют работу этого администратора на своих мониторах (рабочих столах), куда выполняется автоматическое дублирование сессии первого администратора.

Примеры современных средств контроля действий администраторов

В настоящее время на российском рынке представлено достаточно много реализаций систем контроля действий администраторов (СКДА) — программных или программно-аппаратных комплексов, обеспечивающих мониторинг рабочих операций администраторов на предмет их соответствия политике безопасности [9, 10].

К зарубежным СКДА относятся Wallix AdminBastion, Krontech Single Connect, One Identity Safeguard, Indeed Privileged Access Manager, CyberArk Privileged Account Security Solution, Thycotic, ObserveIT. Из отечественных продуктов наибольшую популярность получили такие СКДА, как система контроля действий поставщиков ИТ-услуг (СКДПУ), SafeInspect, Zecurion PAM.

Архитектура большинства из них основана на использовании сервера-посредника как единой точки доступа к функциям администриро-

вания, обеспечивающего усиленную аутентификацию администраторов, контроль доступа, видео-запись графических сессий (RDP, VNC), а также запись текстовых сессий (SSH, Telnet). Кроме того, основная сфера применения подобных СКДА — контроль доступа к АС удаленных администраторов из ИТКС ОП Интернет, что запрещено для критических объектов автоматизации. Но имеются и СКДА, использующие агентов в качестве модулей контроля, что обеспечивает более высокую надежность, универсальность и масштабируемость. Например, схема использования достаточно известной СКДА ObserveIT, представлена на рисунке ниже (рис. 4) [11].

К компонентам СКДА ObserveIT относятся:

1) агенты системы (модули контроля), устанавливаемые на серверы удаленного доступа, локальные серверы, а также АРМ контролируемых администраторов и пользователей, обеспечивающие контроль пользовательских сессий;

2) сервер базы данных (БД), обеспечивающий хранение событий, видеофайлов и метаданных. Данные, хранящиеся на указанном сервере, могут быть использованы для построения отчетов, а также для интеграции с внешними SIEM-системами, а также системами мониторинга сети типа Zabbix, дополняя хранящиеся в них данные;

3) сервер управления, на котором функционирует модуль управления, обеспечивающий администрирование СКДА, сбор событий с агентов системы, а также предоставляющий Web-интерфейс управления системой;

4) АРМ управления (администратора контроля), с которого администратор взаимодействует с модулем управления по сети через графическую консоль, в качестве которой выступает Web-браузер.

СКДА ObserveIT обеспечивает реализацию следующих функций:

1) запись и воспроизведение — видеозапись (для графических сессий) и текстовую запись (для консольных сессий) всей активности контролируемых администраторов и пользователей/(пользователя);

2) формирование интерактивных журналов отчетов — видео и текстовых журналов метаданных для приложений, в том числе для стандартных, облачных и др. приложений. Даже для тех, у которых нет своих внутренних журналов;

3) интеграция с системами SIEM и системами мониторинга сети — обеспечивается простое занесение данных лог-журналов в систему SIEM, систему управления лог-журналами или платформу Zabbix;

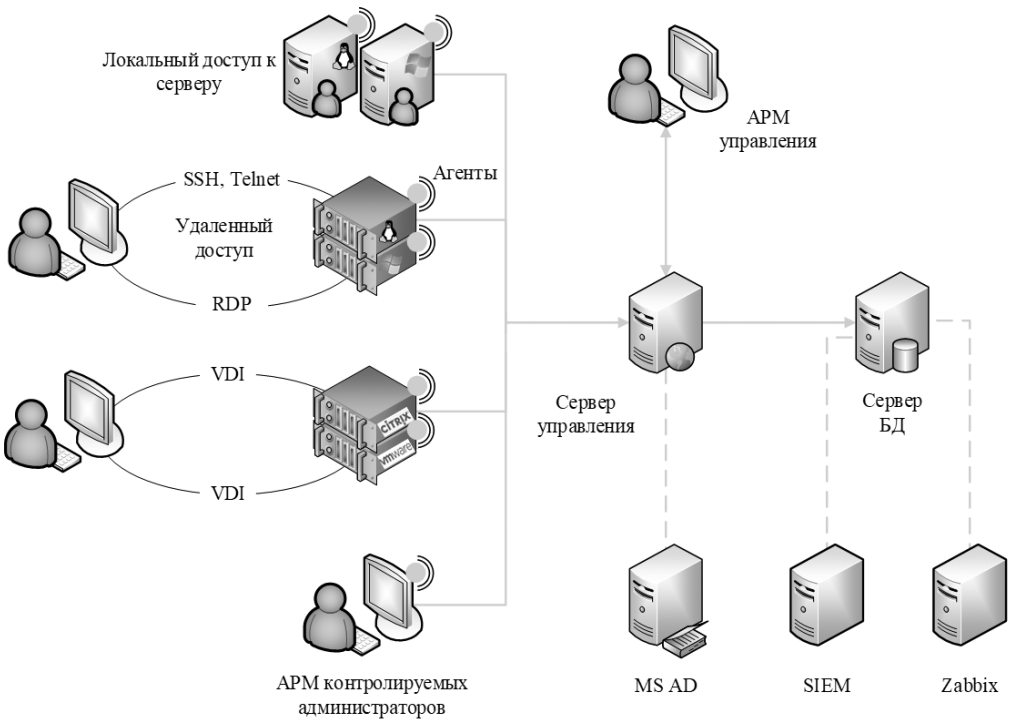

Рис. 4. Схема использования СКДА ObserveIT

4) вывод уведомлений — отображение уведомлений на АРМ управления (администратора контроля) при обнаружении нарушений политики безопасности.

СКДА ObserveIT использует следующие принципы работы:

– распознает сессию и ассоциирует ее с конкретным администратором (пользователем). Как только пользователь начинает сессию, ObserveIT определяет его точный идентификатор (user ID);

– во время сессии все действия администратора (пользователя), вызывающие изменения на экране, записываются в виде последовательности скриншотов, и в дальнейшем могут быть просмотрены в видео-формате. Важно, что в запись попадают только кадры непосредственных изменений на экране. Администратору контроля не нужно тратить время на просмотр видео всей сессии сотрудника (контролируемого администратора);

– параллельно ведутся подробные текстовые журналы метаданных для любых приложений, ресурсов или CLI команд (от англ. Command Line Interface), которые сотрудник использовал. В отличие от обычных системных логов журналы регистрации ObserveIT показывают, что именно делал сотрудник. Информация включает данные об открываемых файлах, окнах и активности пользовательского интерфейса;

– все данные подкреплены видеозаписями. Подробные отчеты отображают все действия, со ссылками на видеозапись. Продуманный интерфейс работы с архивом позволяет легко найти запись действий по временному интервалу, имени учетной записи, приложению, характеру действий.

С учетом того, что в настоящий момент отсутствуют нормативные требования, включая профили защиты к СКДА, то важно, чтобы данное программное средство для возможности использования в АС было сертифицировано по соответствующему уровню контроля отсутствия недекларированных возможностей или уровню доверия. К такому средству относится отечественная СКДА — система контроля действий поставщиков ИТ-услуг (СКДПУ), сертифицированная в МО РФ по 2 уровню контроля отсутствия недекларированных возможностей.

СКДПУ создана российской компанией «АйТи БАСТИОН» и, по сути, является российским аналогом зарубежного продукта Wallix AdminBastion французской компании Wallix, в котором использованы также технологии информационной безопасности ОАО «НПО РусБИТех» — производителя защищенной ОС Astra Linux SE.

Архитектура СКДПУ основана на использовании сервера-посредника (прокси-сервера) как единой точки доступа к функциям администрирования, перехватывающего все сессии контролируемых администраторов по протоколам администрирования RDP, VNC, SSH, Telnet, создающего новые сессии и контролирующего их на предмет соответствия политике безопасности (рис. 5). При этом СКДПУ не требует разверты-

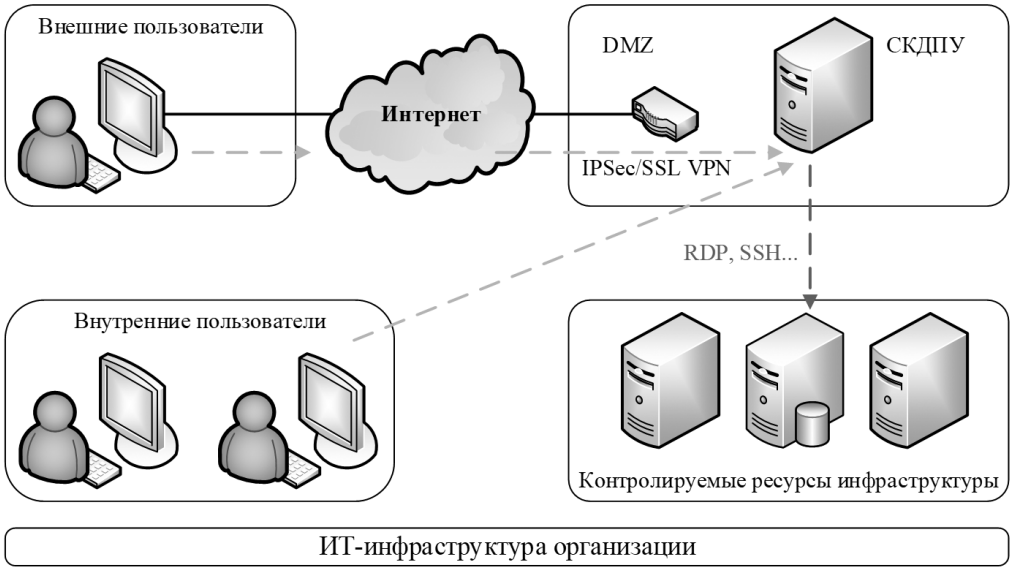

Рис. 5. Схема использования СКДПУ

вания агентов защиты на подконтрольные объекты инфраструктуры — контролируемые администраторы подключаются к серверу посреднику СКДПУ через Web-браузер и получают доступ к конечным управляемым серверам, приложениям или активному сетевому оборудованию через специально сформированные файлы для подключения или настройки.

СКДПУ обеспечивает реализацию следующих функций:

– мониторинг действий пользователей — администраторам контроля предоставляется полная информация о том, кто, как и когда выполнил определенную операцию. Обеспечивается мониторинг подключений к конечным управляемым устройствам и приложениям, а также всех выполняемых действий при администрировании. Консоль администратора контроля позволяет осуществлять мониторинг подключений в реальном времени, а также ретроспективно — для анализа инцидентов информационной безопасности;

– статистика и отчеты о действиях — СКДПУ предлагает стандартные отчеты о глобальной активности (журналы подключений, статистика количества подключений, рейтинг пользователей и т.д.). Дополнительный модуль системы СКДПУ можно использовать для создания статистических отчетов и уведомлений в зависимости от требований нормативных документов;

– запись сеансов — действия, выполняемые на управляемых устройствах, непрерывно записываются для последующего просмотра в формате Flash Video (для графических сеансов RDP и VNC) и в текстовом формате (для сеансов командной строки SSH, Telnet, RS-232). Механизм оптического распознавания символов (OCR) анализирует все графические сеансы Windows и VNC, и позволяет выявлять причину проблем и инцидентов безопасности, фиксируя для сеанса команды, открытые диалоги и использование приложений;

– анализ потока SSH — все вводимые команды анализируются в реальном времени. При обнаружении запрещенных строк можно отправить предупреждение или прервать подключение SSH;

– контроль доступа — контроль доступа к устройствам на основе правил. Правила учитывают различные критерии — такие как IP-адрес, имя учетной записи пользователя, интервал времени, протокол или тип сеанса SSH (X11, Shell, Remote exec и т.д.). Поддерживается разграничение доступа по времени суток и дням недели. Обеспечивается построение политик безопасности при помощи визуального интерфейса;

– контроль в реальном времени — СКДПУ уведомляет администратора контроля о подключениях к управляемым устройствам, определенным как критичные, о неудачной попытке авторизации в СКДПУ или о невозможности автоматического входа с использованием заданной учетной записи;

– формирование цифрового профиля администратора на основании набора его зарегистрированных сценариев и действий. Анализируя полученные данные, СКДПУ составляет карту действий, характерных для каждого отдельного администратора во время работы с управляемыми устройствами и приложениями, и корректирует ее в процессе его дальнейшей работы;

– анализ данных и инцидентов в режиме, приближенном к режиму реального времени, на основе определения аномального поведения пользователей в рамках сессий удаленного доступа, созданием цифровых профилей пользователей с автоматической индикацией уровня доверия к пользователю, основанной на механизмах анализа данных на основе нейронных сетей, алгоритмах статистики и машинного обучения. Анализ различных параметров действий администратора позволяет найти в этих действиях критичные отклонения от его «стандартного поведения»;

– единый вход — каждый пользователь входит в СКДПУ, используя свои учетные данные и пароли, и получает доступ к разрешенным устройствам без повторной авторизации. Пароли для управляемых устройств и приложений хранятся на сервере-посреднике в криптографически хешированном виде, соответственно при успешной первичной аутентификации повторная аутентификация при открытии сессий сервером посредником с управляемыми устройствами выполняется автоматически;

– управление паролями — СКДПУ включает систему управления паролями, которая позволяет автоматически или вручную изменять пароли привилегированных пользователей (например, на серверах Windows и Unix\Linux, а также на ак-

тивном сетевом оборудовании). Предоставляются средства для защищенного хранения учетных данных, ролевого доступа к хранилищу, а также обеспечиваются необходимые механизмы аварийного восстановления на случай возможных отказов (Breaking Glass);

– для организации единой точки входа через несколько серверов-посредников (шлюзов) в СКДПУ реализован дополнительный модуль «Портал доступа», который позволяет в едином Web-интерфейсе использовать все разрешенные пользователю варианты доступа, даже если подключения реализуются через разные физические шлюзы. Модуль оптимизирован для работы, в т.ч. с мобильных устройств, использует клиенты протоколов, реализованные как html5-приложения и позволяет для интеграции в информационные системы использовать открытый протокол обмена данными аутентификации SAML (Security Assertion Markup Language), основанный на языке XML (eXtensible Markup Language).

Платформа СКДПУ доступна в виде готового программно-аппаратного комплекса или виртуального устройства (Virtual Appliance). Для управления СКДПУ достаточно любого современного Web-браузера, например, Firefox из состава ОС Astra Linux SE.

Заключение

В статье рассмотрен практический подход к обеспечению контроля действий администраторов в критически важных АС, основанный на комплексном использовании различных механизмов защиты информации, и раскрыты особенности реализации архитектуры системы контроля действий администраторов. На основе изложенного материала целесообразно сформулировать следующие выводы:

1) наиболее защищенными, надежными, масштабируемыми и отличающимися более низкой сложностью реализации являются СКДА, не требующие разделения управляющего и управляемых сегментов с помощью сервера-посредника. Это связано, прежде всего, с тем, что сервер-посредник легко обойти при наличии у контролируемых администраторов физического доступа к АРМ и серверам в управляемом сегменте, а отсутствие сервера-посредника в «разрыве» сети повышает надежность всей системы защиты и не создает проблем с масштабируемостью сетевой инфраструктуры;

2) СКДА, которые требуют сервера-посредника как единой точки доступа к функциям администрирования, используют, в основном, при контроле доступа к АС удаленных администраторов из ИТКС ОП Интернет, что запрещено для критических объектов автоматизации. В СКДА, построенных по совмещенной архитектуре, при которой используется как сервер-посредник в «разрыве» между управляющим и управляемыми сегментами ЛВС, так и агенты, сервер посредник, как правило, также применяется только для контроля доступа к АС удаленных администраторов из ИТКС ОП Интернет;

3) СКДА без сервера-посредника не требуют доработок для использования в виртуальной среде и совместимости с базовым протоколом доменной аутентификации Kerberos, так как применяется реализация этого протокола на уровне ОС АРМ и серверов, и сервер-посредник не блокирует в «разрыве» сети протокол аутентификации и другие служебные протоколы. При отсутствии сервера-посредника нет необходимости в дополнительной реализации в составе СКДА как стандартных протоколов администрирования, например, RDP, VNC, SSH, так и протоколов администрирования, разработанных для СПО, например, на основе REST API;

4) недостатком СКДА на основе агентов, не требующих разделения управляющего и управляемых сегментов с помощью сервера-посредника, является то обстоятельство, что для максимальной защищенности необходима установка агентов не только на АРМ контролируемых администраторов, но и на всех АРМ и серверах управляемого сегмента, к которым у этих администраторов имеется физический доступ. Но это не снижает их преимущества, так как агенты СКДА могут функционировать в виртуальной среде и быть интегрированы в датчики узловых СОВ или агенты средств антивирусной защиты.

Литература

1. Приказ ФСТЭК России № 235 от 2017 года «Об утверждении требований к созданию систем безопасности значимых объектов критической

информационной инфраструктуры РФ и обеспечению их функционирования».

2. Приказ ФСТЭК России № 239 от 2017 года «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ».

3. Зима В.М., Новиков С.В., Андрушкевич Д.В. Подход к построению защищенных распределенных сетей обработки данных на основе доверенной инфраструктуры // Труды СПИИРАН. — СПб: Наука. 2015. № 1 (38). Т. 1. С. 34–57.

4. Голеусов Я. Обзор технологий, позволяющих контролировать действия привилегированных пользователей [Электронный ресурс]. URL: https://safe-surf.ru/specialists/article/5280/660532/ (дата обращения 20.06.2021).

5. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. — СПб: Наука. 2016. № 45. С. 207–244.

6. Зима В.М., Крюков Р.О. Технология совместного использования квалифицированной и неквалифицированной электронной подписи в системах автоматизированного документооборота специальных ведомств — СПб: Труды ВКА имени А.Ф. Можайского. 2018. № 7 (664). С. 208–216.

7. Методический документ. Меры защиты информации в государственных информационных системах. ФСТЭК России. 2014.

8. Приказ ФСТЭК России № 17 от 2013 года «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» с изменениями, внесенными приказом ФСТЭК России № 27 от 2017 года.

9. Контроль привилегированных пользователей (PAM) [Электронный ресурс]. URL: https://www.anti-malware.ru/security/privileged-access-management (дата обращения 20.06.2021).

10. Головской К.А. Рынок pam в России: краткий обзор // Защита информации. ИНСАЙД — СПб: Издательский Дом Афина. 2017. № 5 (77). С. 54–57.

11. ObserveIT Enterprise [Электронный ресурс]. URL: http://www.infobezpeka.com/products/dlp/ObserveIT_Enterprise/ (дата обращения 20.06.2021).

References

1. Order of FSTEC of Russia № 235 of 2017. «On Approval of Requirements for Creating Security Systems for Significant Objects of Critical Information Infrastructure of the Russian Federation and Ensuring Their Functioning».

2. Order of FSTEC of Russia № 239 of 2017. «On Approval of Requirements for Ensuring the Security of Significant Objects of Critical Information Infrastructure of the Russian Federation».

3. Zima V.M., Novikov S.V., Andrushkevich D.V. Approach to building secure distributed data processing networks based on trusted infrastructure // Proceedings of SPIIRAN — SPb: Nauka. 2015. № 1 (38). T. 1. P. 34–57.

4. Goleusov Y. Review of technologies to control the actions of privileged users [Electronic resource]. URL: https://safe-surf.ru/specialists/article/5280/660532/ (accessed 20.06.2021).

5. Branitskii A.A., Kotenko I.V. Analysis and classification of network attack detection methods // Proceedings of SPIIRAN — SPb: Nauka. 2016. № 45. P. 207–244.

6. Zima V.M., Kryukov R.O. Technology of joint use of qualified and unqualified electronic signature in the systems of automated document flow of special departments. — Saint-Petersburg: Proceedings of A.F. Mozhaisky Military Academy. 2018. № 7 (664). P. 208–216.

7. Methodological document. Information protection measures in state information systems. FSTEC of Russia. 2014.

8. Order of FSTEC of Russia № 17 of 2013. «On Approval of Requirements for Protection of Information Not Constituting State Secrets Contained in State Information Systems» as amended by FSTEC Order № 27 of 2017.

9. Privileged Access Management (PAM) [Electronic resource]. URL: https://www.anti-malware.ru/security/privileged-access-management (accessed 20.06.2021).

10. Golovskoy K.A. Market PAM in Russia: a brief overview // Information Protection. INSIDE — SPb: Athena Publishing House. 2017. № 5 (77). P. 54–57.

11. ObserveIT Enterprise [Electronic resource]. URL: http://www.infobezpeka.com/products/dlp/ObserveIT_Enterprise/ (accessed 20.06.2021).